1. Inject fun, reveal hidden secrets!

Welcome back to the next phase of your journey through the world of Command Injection vulnerabilities, set against the backdrop of our enhanced Asset Discovery tool.

Your mission now is to test the improved security measures and exploit the command injection vulnerability in the `ping` functionality.

Challenge

We're building our Asset Discovery tool and integrating some new features. We've added a security layer, and we think it's more secure now. Can you test it and ensure it's safe?

This challenge focuses on Command Injection. The `ping` input is still vulnerable, but with some added security measures.

- Target Application: Asset Discovery tool
- Initial Endpoint: `http://web0x09.hbtn/app2/`

```
Useful instructions:
1. Log into Asset Discovery tool.
2. ping is vulnerable.
3. We can try and give it an input (google.com for example).
4. To exploit this vulnerability, we need to use Bypass space, Bypass command check.
5. Flag Location is `/etc/1-flag.txt`
```